## Advice on Storing Information in the Cloud

Commercial and free services such as Dropbox offer convenience and simplicity. However, there are risks to their use and it is important that these are understood so that sensible decisions can be made about the suitability of their use for any given purpose.

You should use caution before storing information on Google Apps, Dropbox, or any other cloud service provider. The following issues need consideration:

- The Data Protection Act
- The security of the information
- The criticality of the information
- The value and ownership of the data, and
- The technology required to deliver the service

These areas are considered in more detail below but, as a general rule, ***if there are legal or reputational consequences should the information you are storing be lost, stolen, or seen by unauthorised persons or organisations, you should not use a cloud service provider to store, transmit, or process it***.

### 1 Data Protection and Security

Once data is submitted to the cloud, there are no guarantees as to its security. In fact, there have been many documented examples of security breaches to Dropbox and other cloud services providers. It is an offence under the Data Protection Act to breach the data rights of an individual and you can be held personally liable. Also, bear in mind that many of these cloud storage systems are based in the US and as such subject to US terms and conditions and jurisdiction, perhaps not always compatible with practice in the UK and Europe.

On an individual level cloud services are not subject to the same security measures as used internally. So if you, or someone you share the 'cloud storage' with deletes the document, it may be lost permanently. So do not store the only copy in the cloud!

### 2 Sensitivity

You will need to consider the nature of the information. If it includes sensitive, personal, non-public information (e.g., addresses, financial information, or health information (not exhaustive)) it must **not** be stored in the cloud. If loss or unauthorised access of the data would be in breach of the Data Protection Act, or cause embarrassment or reputational damage to the Authority, again it should **not** be placed with Cloud service providers. Even when using cloud services for non-sensitive information, you should always use a different user name and password to your Authority IT account, and not use your personal cloud storage for Authority documents.

## 3 Criticality

You should also consider the criticality of the data. IT equipment fails, and natural disasters can wipe out entire buildings and cloud service providers rarely give any guarantees about the availability of their services. If you have data that would impact the operation of the Authority in any way should that data be lost or become unavailable, the use of cloud services should be avoided.

## 4 Value and Ownership

Consider the ownership of the data. If you do not own the document i.e. third party reports, or it is copyrighted, you should not place the information with cloud services without their permission.

## 5 Technology

Some cloud technologies require the installation of a local application. The free versions of these are not designed for enterprise use and they can cause issues with the Authority's IT environment. Therefore as a general rule, only the web version of these tools should be used and ICT may be unable to install or support certain applications (including the Dropbox Windows application) where they are known to cause problems to Active Directory. ***ICT / Steria will not install sharing applications on to PCs where they would prevent an unacceptable security risk, or would otherwise interfere with the network.***

## 6 Data Management

The Information you place in the cloud still needs to be managed, and documents should be deleted when no longer required. You should also consider the use of cloud storage and try to avoid the proliferation of multiple accounts. Managers should ensure that when staff leave they clear / delete the account, as we would with internal access. Cloud services are available from anywhere so when staff leave they can still gain access to the documents whether they are employed by us or not.

## 7 Terms and Conditions

Many of the free cloud storage solutions are designed for home use, and may not be free for organisations, and some services require you to sign up on behalf of an organisation. So please make sure you check the Terms and Conditions and have the authority to agree to them.

If you have any questions about whether cloud storage (at Dropbox or any service provider) is an appropriate tool for your storage needs, please contact the Steria Service Desk or the Data Protection Officer.